

REMARKS

Claims 1-17, 20, and 22-33 are pending and stand rejected. Claim 33 is canceled and claim 34 is added. No claims are amended.

Claim Rejections under 35 U.S.C. § 103

Claims 1-10, 12-17, and 20-33 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Bates et al., U.S. Patent 6,721,721 in view of Hericourt et al., U.S. Patent 7,099,916. Claim 11 stands rejected as being unpatentable over the combination of Bates and Hericourt in view of Symantec, "Norton AntiVirus Corporate Edition." Applicants respectfully traverse these rejections as applied to the current claims.

The claimed invention uses a virus outbreak report indicating a virus attack to compute a computer virus alert time. The computer virus alert time is compared with a time stamp corresponding to an earliest moment or first time computer code was allowed to execute on a computer coupled to a computer network, and the executability of the computer code is determined in response to the comparison. Specifically, most of the independent claims recite limitations corresponding to:

entering a first computer virus status mode in response to a first computer virus outbreak report indicating a virus attack threat to a computer network;
computing a first computer virus alert time corresponding to entry into the first computer virus status mode;
comparing a time stamp of executable computer code corresponding to an earliest moment the computer code was allowed to execute on a computer coupled to the computer network with the first computer virus alert time; and
determining the executability of the computer code in response to the result of the comparing step.

(quoting from claim 1). Dependent claim 8 further recites that the “computer code is determined to be executable only when the computer code is time stamped prior to the first computer virus alert time.” In other words, the computer code is executable because it has existed since before the virus alert and, therefore, is unlikely to be infected by that virus.

New independent claim 34 resembles claim 1, except that the time stamp of the executable computer code corresponds “to a *first time* the computer code was allowed to execute on a computer coupled to the computer network.” Support for claim 34 is found throughout the specification, including at paragraphs 38, 50, and 75. Paragraph 38 states that the “time stamp of an executable computer code corresponds to an earliest moment this particular computer code was allowed to execute by computers 2,3 on the network.” Paragraph 50 states that “memory table 205 stores hash values of computer codes that have been executed and a time entry recording the time of inserting the hash value into memory table 205.” Paragraph 75 describes how the access control module 203 assumes that computer code requesting execution has never been allowed to execute if the code’s hash value is not found in the memory table. Thus it is apparent that the time stamp corresponds to the first time the computer code was allowed to execute.

As Applicants previously discussed, the cited references, at the least, fail to disclose the claimed time stamp. Bates discloses a system that integrates virus checking functionality into a computer database search environment, thereby allegedly decreasing the risks of viruses associated with accessing search results from computer database searches. See Bates, Abstract; column 3, lines 1-3. At col. 9, line 56 – col. 10, line 8, Bates describes how the user can assess the “trustworthiness” of a search result file by setting a virus criterion as to (i) whether the file has been virus checked within a predetermined period of time; (ii) whether the file has been

changed since the last time a virus check was performed; or (iii) whether a particular period of time has elapsed in which the file has been found to be free of viral infection. Thus Bates at most discloses use of a single time stamp indicating the time the file was last checked for a virus.

The Examiner acknowledges that Bates does not explicitly disclose that the time stamp corresponds to an execution time of the computer code. The Examiner addresses this lack of disclosure by citing to Hericourt, which allegedly discloses that virus scanning of executable code can comprises an execution of the code. Therefore, the Examiner alleges, it would have been obvious to one of ordinary skill in the art to recognize the teachings of Hericourt within the system of Bates. Hericourt does not disclose or suggest using timestamps to determine the executability of computer code.

Neither Bates nor Hericourt discloses or suggests using a time stamp that corresponds to an earliest moment the computer code was allowed to execute on a computer coupled to a computer network. Even if Bates discloses a time stamp indicating when code was virus scanned, and the scanning comprised an execution as allegedly taught by Hericourt, there is no teaching or suggestion that the time stamp corresponds to an earliest moment that the code was scanned or executed. Both references assume that code is scanned multiple times, and neither reference attaches any special significance to an earliest moment (or first time) that the code was scanned or executed. Rather, the time stamp in the references represents the latest time the code was scanned or executed.

The Examiner's remarks in the Office Action do not justify the rejection of the claims. In the specific rejection of claim 1, the Examiner states that "Hericourt teaches that virus scanning of executable code comprises an execution of the code, and therefore 'an earliest moment' the code is allowed to execute" and cites to col. 3, lines 25-54. However, this portion of Hericourt

simply describes the numerous ways a virus can be detected and merely mentions that code can be emulated during virus scanning. There is no teaching or suggestion that a timestamp corresponds to an earliest moment the code is allowed to execute.

The Examiner's remarks in the "Response to Arguments" section also fail to justify the rejection. The Examiner first makes the noncontroversial assertions that code can be executed multiple times, and that the combination of Bates and Hericourt enable the execution of computer code on a computer coupled to a network. The Examiner's next point is that:

...out of the multitude of instances a particular piece of computer code is executed, either via scanning or via end-user execution, the timestamp associated with the virus check for that computer code represents "an earliest execution time" in comparison to subsequent instances of execution for that piece of computer code.

(Office Action, page 18 lines 2-6).

This statement, however, misses the point and does not explain why the combination of the references would render the claims obvious. The Examiner states that a timestamp can represent the earliest execution with respect to subsequent executions, but there is no basis for arbitrarily excluding from consideration any executions that occur before the so-called "earliest" execution associated with the timestamp. In other words, a particular timestamp in Bates cannot be said to represent the "earliest" execution because there are an arbitrary number of executions that occur before and after the execution represented by the timestamp. Therefore, a person of ordinary skill in the art considering the teachings of Bates and Hericourt would not find the claimed invention obvious.

The Symantec reference fails to remedy the deficiencies of Bates and Hericourt described above. Therefore, a person of ordinary skill in the art, considering the teachings of the references either alone or in combination would not find the claimed invention obvious.

CONCLUSION

Accordingly, Applicants respectfully submit that the pending claims are allowable over the cited references and request allowance of the claims. If the Examiner believes that direct contact with the Applicants' attorney will advance the prosecution of this case, the Examiner is encouraged to contact the undersigned as indicated below.

Respectfully submitted,

CAREY S. NACHENBERG, ET AL.

Dated: April 10, 2008

By: /Brian Hoffman/
Brian M. Hoffman, Reg. No. 39,713
Attorney for Applicants
Fenwick & West LLP
801 California Street
Mountain View, CA 94041
Tel.: (415) 875-2484
Fax: (415) 281-1350